Examples of Pharmacy HIPAA Violations

July 8, 2025
By Michael H. Cohen

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law enacted in 1996 to protect patients' private health information (PHI). HIPAA establishes rules around how healthcare providers, including pharmacies, store, use, and share sensitive health data.

Due to their direct access to sensitive data, pharmacies are especially vulnerable to HIPAA violations and enforcement actions. **Common examples of pharmacy HIPAA violations include improper disclosure of PHI, failure to secure electronic records, and inadequate staff training.**

This blog will give a quick overview of HIPAA and its role in healthcare and how it applies to pharmacies. It will then share common examples of pharmacy HIPAA violations.

What Is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law enacted in 1996 to protect individuals' health information and ensure patient privacy. Overseen by the U.S. Department of Health and Human Services (HHS) and enforced by the Office for Civil Rights (OCR), HIPAA established national standards for safeguarding Protected Health Information (PHI) across the healthcare system.

Two key HIPAA rules are especially relevant to pharmacies:

- **The HIPAA Privacy Rule:** This rule regulates how covered entities, such as pharmacies, healthcare providers, health plans, and healthcare clearinghouses, may use and disclose a patient's protected health information. It ensures that only the minimum amount of information necessary is shared, and that patients are aware of and can control how their health records are used.
- **The HIPAA Security Rule:** This rule requires pharmacies to implement security measures to protect electronic PHI (ePHI) from unauthorized access, loss, or tampering. This includes technical, physical, and administrative safeguards for medical records and prescriptions.

Because pharmacies regularly handle health information, maintain prescription bottles, and process data for insurance companies, maintaining HIPAA compliance is important. Violating HIPAA can lead to civil penalties, corrective action plans, and even court orders.

Does HIPAA Apply to Pharmacies?

Yes, **HIPAA applies to all pharmacies**. As covered entities, both large chain businesses (like CVS Pharmacy and Walgreens) and small pharmacies must comply with HIPAA requirements. They are responsible for safeguarding every patient's PHI, whether in paper or electronic form. Pharmacy staff, including pharmacists and technicians, must follow internal monitoring, procedures, and policies to ensure they do not disclose PHI without patient authorization or a valid court order.

HIPAA governs how pharmacies collect patient information, share health insurance details with insurers, and store psychotherapy notes and medical records. They also govern processing and labelling prescriptions to protect privacy.

What Happens When a Pharmacy Violates HIPAA?

When a pharmacy violates the Health Insurance Portability and Accountability Act (HIPAA), the consequences can be severe, both legally and financially. Legal and financial penalties for HIPAA violations in pharmacies vary depending on the nature and severity of the breach. **Civil penalties can range from $100 to $50,000 per violation, with annual maximums reaching up to $1.5 million for each category of violation.**

In some cases, especially those involving willful neglect or intentional misconduct, criminal charges may also apply. Pharmacies found in violation may be required to undergo a corrective action plan (CAP), which typically involves overhauling internal policies, retraining staff members, and committing to ongoing compliance monitoring.

HIPAA violations don't just bring fines; they also **erode patient trust and tarnish the pharmacy's reputation.** Patients rely on healthcare providers, including pharmacies, to keep their health records and personal information confidential. When a violation occurs, such as an employee accessing medical records without patient authorization or improperly disposing of prescription bottles with visible labels, it can severely undermine confidence in the pharmacy's ability to protect patient privacy. Even a single breach may lead to public backlash, negative media coverage, and loss of customer loyalty.

Real-world examples underscore how seriously HIPAA enforcement is taken. CVS Pharmacy, for instance, paid a $2.25 million settlement after it was discovered that several of its locations improperly disposed of pill bottles and patient information in unsecured trash bins.

The long-term risks of ignoring HIPAA compliance extend far beyond initial fines. **Pharmacies that do not take HIPAA requirements seriously may face the revocation of their operating licenses, the loss of contracts with health plans and insurance companies, and increased vulnerability to lawsuits.** Regulatory scrutiny can also intensify, leading to frequent audits and mandatory internal monitoring. Over time, failure to enforce privacy rule requirements, train staff, and implement proper security measures can compromise a pharmacy's ability to operate effectively and legally.

To avoid these risks, pharmacies must treat HIPAA compliance as a non-negotiable part of their business operations. Every member of the pharmacy staff, from technicians to pharmacists, plays a role in protecting patient information. If your pharmacy is uncertain about its compliance status or has experienced a potential violation, now is the time to act.

7 Examples of Pharmacy HIPAA Violations

Below are seven common examples of how pharmacy staff can violate HIPAA and put both patients and the pharmacy at risk:

Unauthorized Access to Patient Information

One of the most frequent HIPAA violations in pharmacies involves employees accessing health records without a valid reason. **Under the HIPAA Privacy Rule, only authorized personnel with a legitimate work purpose may view or handle a patient's protected health information.**

However, violations occur when staff members access medical records out of curiosity, such as looking up a family member's or celebrity's prescriptions, as seen in the Britney Spears case. These actions violate not only HIPAA rules but also patients'

rights and privacy.

Improper Disposal of Patient Records

Improperly discarding prescription bottles, patient records, or printed health information can lead to serious compliance issues. **HIPAA requires that health care providers, including pharmacies, implement secure procedures for destroying PHI.**

Throwing away prescription labels or documents without shredding or placing them in unlocked trash bins, as seen in the high-profile CVS Pharmacy settlement, can expose sensitive data. Such incidents often result in OCR investigations, corrective action plans, and fines for failing to make reasonable efforts to protect patient information.

Sharing Patient Information Without Consent

Discussing PHI in public areas where others can overhear, or disclosing it to unauthorized individuals, constitutes an impermissible disclosure under the privacy rule. For example, talking about a patient's medications at the counter loud enough for others to hear violates their confidentiality.

Additionally, sharing PHI with an insurance company, family member, or other third party without proper patient authorization breaches HIPAA requirements. These incidents often trigger complaints to the human services office or direct OCR investigation.

Failure to Secure Electronic Records

HIPAA's Security Rule requires covered entities to adopt technical security measures to safeguard electronic health information (ePHI). Unfortunately, many pharmacies, especially small pharmacies, fall short by failing to secure their computer systems.

Leaving terminals unlocked, using weak passwords, or not implementing proper internal monitoring exposes patient data to theft or unauthorized access. Inadequate protection of electronic PHI is one of the most common potential violations pharmacies face.

Misuse of Fax or Email for Sending PHI

Transmitting health information by fax or email without proper safeguards is another frequent cause of violating HIPAA. **For example, sending PHI to the wrong recipient, such as the incorrect fax number or email address, or failing to use encryption, are clear HIPAA violations.** Despite being common tools for health care providers, fax and email systems must follow HIPAA standards to prevent breaches of health information (PHI) and reduce the risk of impermissible disclosure.

Lack of Proper Staff Training

HIPAA requires that pharmacy staff receive ongoing training about privacy and security obligations. However, a lack of proper education results in employees unknowingly mishandling PHI, failing to follow procedures, or breaching patient privacy. When staff don't fully understand their role in HIPAA compliance, they may accidentally disclose PHI or fail to implement necessary policies and procedures, leaving the pharmacy vulnerable to audits and penalties.

Inadequate Physical Security Measures

Failing to physically secure areas where patient information is stored, like leaving unlocked filing cabinets, unattended prescription bags, or exposing records to unauthorized personnel, can result in civil rights violations under HIPAA. These HIPAA privacy rule breaches are especially dangerous in high-traffic areas such as the health center, department office, or pharmacy consultation counters. Proper compliance requires pharmacies to implement safeguards that protect health records from both physical and digital threats.

How to Stay Compliant With Pharmacy HIPAA Regulations

Staying compliant with HIPAA regulations is essential for any pharmacy that handles protected health information (PHI). To maintain HIPAA compliance, **pharmacies must implement clear and consistent policies and procedures that align with both the HIPAA Privacy Rule and Security Rule**. Best practices include assigning a designated HIPAA compliance officer, conducting regular risk assessments, and establishing protocols for secure data handling. Regular self-audits, proper documentation, and active monitoring are key to identifying weaknesses before they result in civil penalties or an OCR investigation.

Start by identifying all areas where patient information is handled. From there, create and enforce written privacy policies that limit PHI access to authorized staff members only. Pharmacies should also **develop breach notification procedures, require patient authorization when needed, and comply with state laws in addition to federal rules.** Establishing secure disposal methods for medical records, maintaining minimum necessary use policies, and monitoring for potential impermissible disclosures are also critical.

Typically, a pharmacy's ability to protect patient privacy depends heavily on its employees. **Every team member, from pharmacists to technicians, must receive comprehensive HIPAA training upon hiring and at regular intervals thereafter.** This training should cover how to properly access health records, secure PHI, and avoid actions that could violate HIPAA, such as discussing prescriptions in public areas or accessing psychotherapy notes without cause.

Additionally, **implement security measures** such as locked cabinets, password-protected computers, and monitored access to sensitive files. Educating staff not only reduces risk but also strengthens your pharmacy's overall compliance posture

Furthermore, modern pharmacies rely on technology to manage patient records, process prescriptions, and communicate with healthcare providers and insurance companies. While convenient, this digital landscape presents new risks if not properly managed. **To stay compliant, ensure that all electronic systems handling PHI are encrypted, password-protected, and backed by access controls**. Use secure portals for transmitting PHI, never send sensitive data via unencrypted email, and verify fax numbers before transmission. Regular updates, anti-virus protections, and secure networks are vital for defending against unauthorized access or breaches.

Given the complexity of HIPAA rules, **working with a healthcare attorney who understands the accountability act, federal regulations, and real-world enforcement is a smart move for any pharmacy**. An experienced HIPAA attorney can help implement compliant procedures, guide staff training, and represent your interests if an OCR investigation or enforcement action occurs.

They can also interpret regulatory updates, address potential violations, and advise on handling court orders, patient complaints, or compliance audits. With legal guidance, your pharmacy can go beyond just meeting minimum standards – it can operate with confidence.

What to Do if Your Pharmacy Is Not HIPAA Compliant

The first step is to **identify the source and scope of the compliance issue**. Whether it involves patient records, mishandled prescription bottles, unsecured electronic PHI, or untrained pharmacy staff, act quickly to contain the situation.

You should immediately cease any activity that could further compromise patient privacy and secure any data that may have been at risk. Conduct a preliminary internal review and document everything. This shows the Office for Civil Rights (OCR) that you're taking the issue seriously and making reasonable efforts to correct it.

Once a HIPAA violation is identified, you must assess whether it qualifies as a reportable breach under the HIPAA Breach Notification Rule. **If it does, you are required to notify affected individuals, the Department of Health and Human Services (HHS), and in some cases, the media.** It's important to notify individuals promptly within 60 days of discovering the breach, and to provide clear information about what occurred, what data was affected, and what steps the pharmacy is taking

in response. Failure to follow these steps can lead to an enforcement action and a mandatory corrective action plan.

Bringing your pharmacy back into compliance means implementing both short-term fixes and long-term system improvements. **This includes updating your policies and procedures, strengthening security measures (physical and digital), and improving how PHI is accessed, stored, and shared**. Your pharmacy may also need to consult with a healthcare attorney to navigate the process and respond to government inquiries.

If your pharmacy has experienced a breach, you must follow federal guidelines for reporting. **For minor incidents involving fewer than 500 individuals, you can submit an annual report to HHS through the OCR Breach Portal. For breaches affecting 500 or more individuals, you must report the incident within 60 days of discovery and notify local media outlets as required by law.** In both cases, maintaining detailed records of how the breach was handled and the corrective actions taken is essential. Transparency and cooperation during this process will help demonstrate your pharmacy's commitment to HIPAA compliance and may mitigate the risk of heavier civil penalties.

In some cases, patients, staff members, or other concerned individuals may wish to file a complaint about a potential violation. Complaints can be submitted directly to the Department of Health and Human Services' Office for Civil Rights via the HHS website. Pharmacies should take every complaint seriously, even if it seems minor, and respond appropriately.

A complaint can trigger an OCR investigation, which may uncover other compliance issues. Being proactive about resolving complaints internally, conducting a thorough review, and maintaining compliance documentation can help prevent escalation.

Want to Avoid HIPAA Violations and Stay Compliant?

As covered entities, pharmacies are on the front lines of handling sensitive health information, and even a small oversight can lead to costly violations, legal penalties, and damage to your reputation. **Now more than ever, pharmacies must remain vigilant.**

From securing patient records to training staff and properly handling prescriptions, every action matters. Patients, too, should feel empowered to ask questions and understand how their protected health information (PHI) is being used and protected.

If you're unsure whether your pharmacy is truly HIPAA compliant or you've recently experienced a potential violation, it's time to take proactive steps with the right legal support.

FAQ About Pharmacy HIPAA Violations

Below are common questions and clear answers about how HIPAA applies in pharmacy settings:

Are Pharmacies Covered Entities Under HIPAA?

Yes, pharmacies are considered covered entities under HIPAA and must follow all privacy and security rules to protect patient information. They are legally required to handle PHI in compliance with federal regulations.

What Are Common HIPAA Violations in Pharmacies?

Common violations include unauthorized access to patient records, improper disposal of prescription bottles, unsecured electronic systems, and sharing patient information without consent. These actions can result in civil penalties and OCR investigations.

How Can Patients Protect Their Privacy at the Pharmacy?

Patients should avoid discussing sensitive medical information aloud and ask how their health information is stored and shared. They can also request a copy of the pharmacy's HIPAA privacy practices.

Can Pharmacy Employees Access Any Patient Information?

No, pharmacy employees can only access PHI when necessary for their job duties. Accessing information out of curiosity, such as looking up a friend or celebrity, is a HIPAA violation.

What Should I Do if I Suspect My Pharmacy Violated HIPAA?

You can report the incident to the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS). Filing a complaint can lead to an official investigation and corrective actions.

How Often Should Pharmacies Conduct HIPAA Training?

HIPAA training should be conducted upon hire and regularly thereafter, typically once a year. Ongoing education ensures staff members understand evolving HIPAA rules and how to avoid violations.

Are Electronic Prescriptions Covered Under HIPAA?

Yes, electronic prescriptions are considered electronic PHI (ePHI) and are fully protected under the HIPAA Security Rule. Pharmacies must use secure systems and encryption to protect this data.